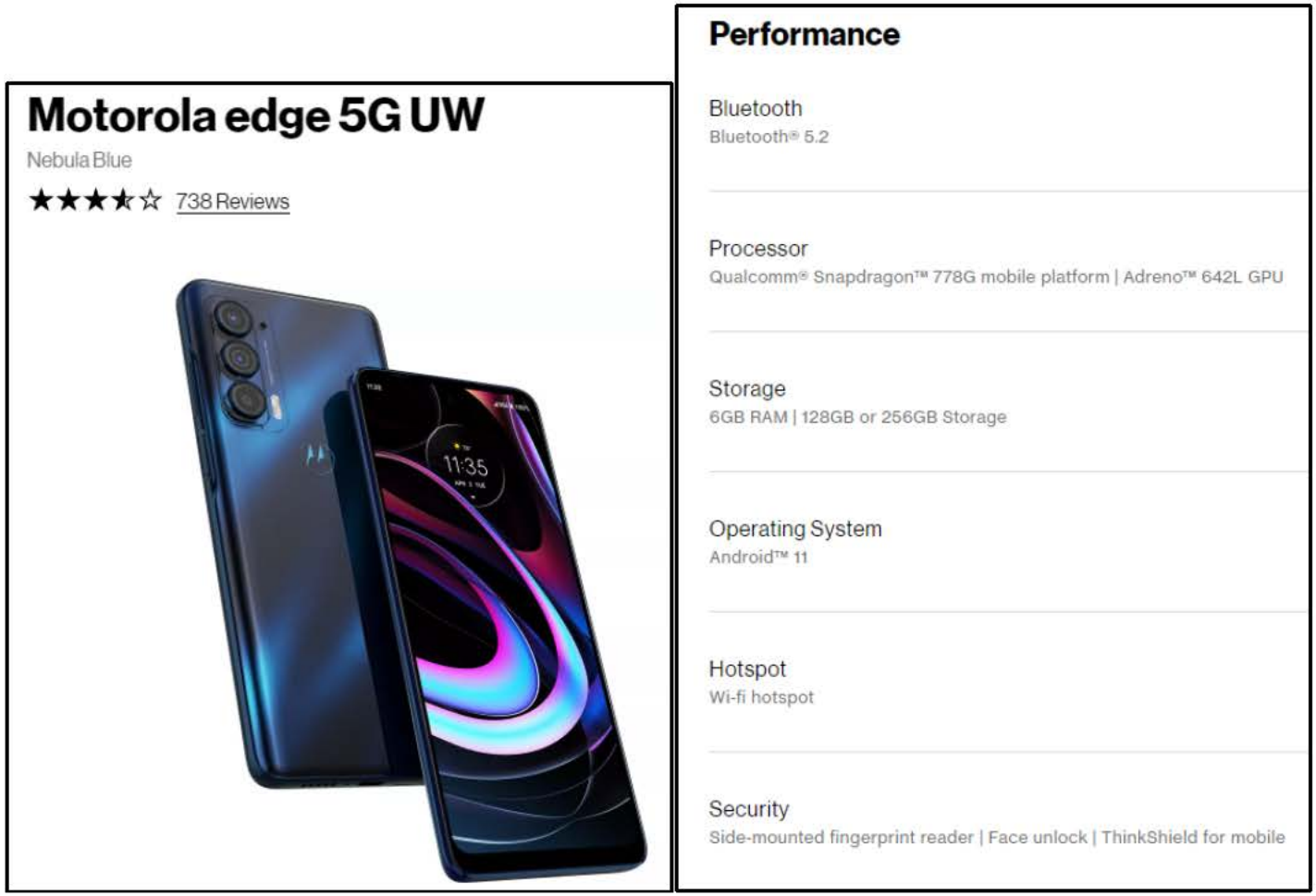
EXHIBIT 18

U.S. Patent No. 7,930,539

Claim 1	Identification
1[pre] A computer-implemented method for use in a computer system including a plurality of resources, the method comprising steps of:	To the extent the preamble is limiting, the Lenovo moto Edge 5G uses an ARMv8-A based processor that implements a method for use in a computer system including a plurality of resources comprising the steps below. 

Claim 1	Identification

https://www.verizon.com/smartphones/motorola-edge-5g-uw/

Moto edge 5G includes a Qualcomm Snapdragon 778G mobile platform processor, which uses the Qualcomm Kryo 670 CPU.
Snapdragon 778G 5G Mobile Platform | Qualcomm

Kryo 670 [edit]

The Kryo 670 CPU was announced with the Snapdragon 780G on 25 March 2021.[39] It is also used in the Snapdragon 778G and 778G+, as well as the 782G.

- 1 Kryo 670 Prime (ARM Cortex-A78 based) @ 2.4-2.7 GHz
- 3 Kryo 670 Gold (ARM Cortex-A78 based) @ 2.2 GHz
- 4 Kryo 670 Silver (ARM Cortex-A55 based) @ 1.9 GHz
- 778G/778G+/782G: TSMC 6 nm (N6) Process
- 780G: Samsung 5 nm LPE Process

https://en.wikipedia.org/wiki/Kryo

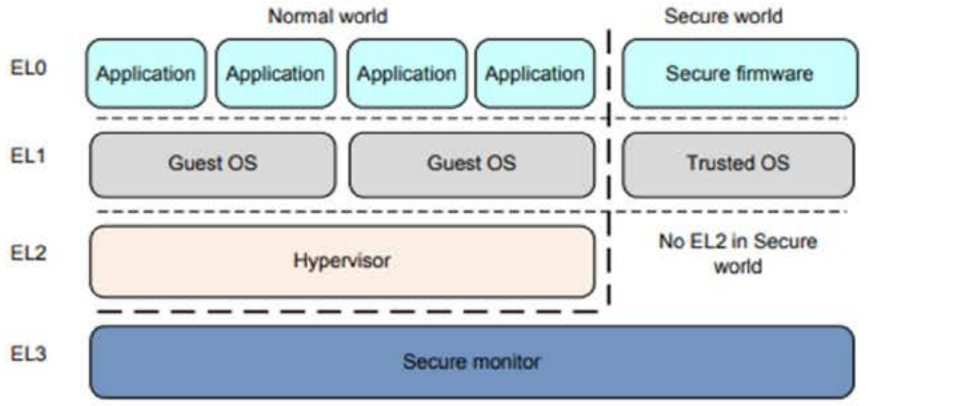
The Cortex-A55 core is a mid-range, low-power core that implements the ARMv8-A architecture with support for the v8.2 extension, the RAS extension, the Load acquire (LDAPR) instructions introduced in the ARMv8.3 extension, and the Dot Product instructions introduced in the ARMv8.4 extension.

ARM® Cortex®-A55 Core, Revision r1p0, Technical Reference Manual

1 Security in an ARMv8-A system

A secure or trusted system is one that protects assets, for example passwords or credit card details from a range of plausible attacks, to prevent them from being copied or damaged, or made unavailable.

Security is defined by the principles of:

Claim 1	Identification
	Security in an ARMv8-A System (https://developer.arm.com/documentation/100935/0100/Security-in-ARMv8-A-systems-?lang=en)
[1] (A) receiving a request from a software program to access a specified one of the plurality of resources;	The system receives a request from a software program (such as a software application or OS) to access a resource, such as a normal world resource or a secure world resource.  Figure 1 Security model for AArch64 The ARM Architecture Reference Manual uses the terms Secure and Non-secure to refer to system security states. A Non-secure state does not automatically mean security vulnerability, but rather normal operation and is therefore the same as the Normal world. Typically, there is a master and slave relationship between Non-secure and Secure worlds. Code in the Secure world is only executed when the OS permits Secure world execution through a mechanism that is initiated by the Secure Monitor Call (SMC) instruction. Security in an ARMv8-A System at 5
[1] (B) determining whether the specified one of the plurality of resources is a protected resource;	A determination is made whether the specified one of the plurality of resources is a protected resource. For example, whether the resource is in secure world or normal world.

Claim 1	Identification
	The ARM Security Extensions model allows system developers to partition device hardware and software resources, so that they exist in either the Secure world for the security subsystem, or the Normal world for everything else. Correct system design can ensure that no Secure world assets can be accessed from the Normal world. A Secure design places all sensitive resources in the Secure world, and ideally has robust software running that can protect assets against a wide range of possible software attacks. Security in an ARMv8-A System at 5
[1] (C) if the specified one of the plurality of resources is a protected resource, performing steps of:	If the specified one of the plurality of resources is a protected resource (e.g., in secure world), the steps below are performed.
[1(C)] (1) if the computer system is operating in a protected mode of operation, then denying the request regardless of access rights associated with the software program including software programs having a most-privileged level; and	If the computer system is operating in a protected mode of operation, then the request is denied regardless of access rights associated with the software program including software programs having a most-privileged level. For example, if the Secure Monitor Disable bit is set to disable, Secure Monitor Call (SMC) instructions, required to access secure world resources, are disabled. **D19.2.120 SCR_EL3, Secure Configuration Register** The SCR_EL3 characteristics are: **Purpose** Defines the configuration of the current Security state. It specifies: • The Security state of EL0, EL1, and EL2. The Security state is Secure, Non-secure, or Realm. • The Execution state at lower Exception levels. • Whether IRQ, FIQ, SError interrupts, and External abort exceptions are taken to EL3. • Whether various operations are trapped to EL3. Arm Architecture Reference Manual for A-Profile Architecture at D19.2.29 (https://developer.arm.com/documentation/ddi0487/latest/)

Claim 1	Identification

SMD, bit [7]

Secure Monitor Call disable. Disables SMC instructions at EL1 and above, from any Security state and both Execution states, reported using an ESR_ELx.EC value of 0x00.

0b0 SMC instructions are enabled at EL3, EL2 and EL1.

0b1 SMC instructions are UNDEFINED.

Note

SMC instructions are always UNDEFINED at EL0. Any resulting exception is taken from the current Exception level to the current Exception level.

If HCR_EL2.TSC or HCR.TSC traps attempted EL1 execution of SMC instructions to EL2, that trap has priority over this disable.

The reset behavior of this field is:

- On a Warm reset, this field resets to an architecturally UNKNOWN value.

Arm Architecture Reference Manual for A-Profile Architecture at D19-6959.

The *Secure Monitor Call* (SMC) instruction provides software with a system call to EL3. When executing at a privileged Exception level, SMC instructions generates exceptions. For more information, see *Secure Monitor Call (SMC) exception* on page G1-9811 and *SMC* on page F5-8734.

Figure G1-1 shows that when EL3 is using AArch32, the Exception levels and modes available in each Security state are as follows:

Secure state

EL0 User mode.

EL3 Any mode that is available in Secure state, other than User mode.

Arm Architecture Reference Manual for A-Profile Architecture at G1-9748-49.

Claim 1	Identification
[1(C)] (2) processing the request based on the access rights associated with the software program if the computer system is not operating in the protected mode of operation.	If the computer system is not operating in the protected mode of operation (e.g., SMD set to 0), then the request is processed based on access rights associated with the software program. The ARM Architecture Reference Manual uses the terms Secure and Non-secure to refer to system security states. A Non-secure state does not automatically mean security vulnerability, but rather normal operation and is therefore the same as the Normal world. Typically, there is a master and slave relationship between Non-secure and Secure worlds. Code in the Secure world is only executed when the OS permits Secure world execution through a mechanism that is initiated by the Secure Monitor Call (SMC) instruction. **Note** The use of the word world is used to describe not just the Execution state, but also all memory and peripherals that are accessible in that state. Non-secure memory and functions are also accessible to the Secure world. The role of the Secure monitor is to provide a gatekeeper which manages the switches between the Secure and Non-secure worlds. In most designs its functionality is similar to a traditional operating system context switch, ensuring that state of the world that the core is leaving is safely saved, and the state of the world the processor is switching to is correctly restored. Security in an ARMv8-A System at 5